Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 13 February 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- SecurityFocus reports a previously−unknown software flaw in a widely−deployed General Electric energy management system contributed to the devastating scope of the August 14th northeastern U.S. blackout. (See item 1)
- The Associated Press reports two dozen countries, led by the Australian Competition and Consumer Commission, are participating in a three−day crackdown on scam Websites that try to swindle visitors with get−rich−quick and other schemes. (See item 10)
- The Associated Press reports the District of Columbia Water and Sewer Authority plans to spend millions to eradicate the high lead levels, as evidenced by tests on some city water samples. (See item 19)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *February 12, SecurityFocus* — **Software bug contributed to blackout. A previously−unknown software flaw in a widely−deployed General Electric energy management system contributed to the devastating scope of the August 14th northeastern U.S. blackout, industry officials said this week.** The bug in GE Energy's XA/21 system was discovered in an intensive code audit conducted by GE and a contractor in the weeks following

the blackout, according to FirstEnergy Corp., the Ohio utility where investigators say the blackout began. **The flaw was responsible for the alarm system failure at FirstEnergy's Akron, OH control center that was noted in a November report from the U.S.−Canadian task force investigating the blackout. The XA/21 bug was triggered by a unique combination of events and alarm conditions on the equipment it was monitoring,** FirstEnergy spokesperson Ralph DiNicola DiNicola said. When a backup server kicked−in, it also failed, unable to handle the accumulation of unprocessed events that had queued up since the main system's failure. FirstEnergy says it already patched the blackout bug last fall, when GE made a fix available, and is in the process of replacing the XA/21 with a competing system −− a changeover that was planned before the blackout.
Source: http://www.theregister.co.uk/content/53/35511.html

2. *February 12, Reuters* — **Department of Energy sets oil stockpile contracts. The Department Energy said Thursday it awarded new contracts to deliver 104,000 barrels per day (bpd) of crude oil to the Strategic Petroleum Reserve under a royalty−in−kind program.** The contracts were awarded for six months, beginning in April, the government said. The crude oil will come from exchange arrangements the companies make for crude from federal offshore leases in the Gulf of Mexico and owed to the U.S. government. About 643 million barrels of oil are currently stored in the nation's stockpile.
Source: http://biz.yahoo.com/rc/040212/energy_stockpile_1.html

3. *February 11, Federal Energy Regulatory Commission* — **Interagency agreement to coordinate review of LNG terminal safety and security signed. The Federal Energy Regulatory Commission, Coast Guard and Department of Transportation Wednesday announced an interagency agreement to provide for the comprehensive and coordinated review of land and marine safety and security issues at the nation's liquefied natural gas (LNG) import terminals.** The agreement clearly delineates the roles and responsibilities of each agency relative to LNG terminals and LNG tanker operations, and stipulates that the agencies identify issues early and quickly resolve them. The agreement reinforces the agencies' working relations in coordinating the seamless review of safety and security issues that may arise from the movement of LNG tankers, the transfer of the LNG to the terminal, and terminal operations. Further, the agencies agree to build a consensus on any hazard studies or other documents that may include safety and security analyses. Agreement: http://www.ferc.gov/industries/gas/indus−act/LNG−Safety−Agre ement.pdf
Source: http://www.ferc.gov/press−room/pr−current/02−11−04−interagen cy.asp

4. *February 11, Nuclear Regulatory Commission* — **Search under way for radioactive sources missing from New Jersey site. Two sealed sources of radioactive material from a damaged moisture density gauge have been reported missing from an East Orange, NJ, construction site.** The Nuclear Regulatory Commission (NRC) has sent inspectors to the site in response to the loss of the sources, which was reported to the NRC on Monday, February 9. **While the amount of radioactive material involved is not significant, any individuals having direct contact with one or both of the radioactive sources for a prolonged period of time could potentially receive harmful amounts of radiation exposure.** The sources −− one holding 11 millicuries of cesium−137 and the other holding 40 millicuries of americium−241 −− are less than an inch in diameter. At about noon on Monday, the gauge's operator left the area where the device was located. When the operator returned at about 12:35 p.m., the crushed

remains of the gauge were found. However, most of the device could not be found, most importantly the two radioactive sources.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2004/04−0 04i.html

5. *February 11, Associated Press* — **Workers shut down construction at liquid natural gas plant in Trinidad. Protesting workers in southwest Trinidad on Wednesday shut down a construction project at a liquid natural gas plant that supplies the United States with more than three−fourths of its natural gas imports, a company spokesperson said. Production was not affected by the protest because the construction site is separate from normal operations,** Atlantic LNG spokesperson Esther Le Gendre said. At around dawn Wednesday, about 50 workers locked the gates to the construction site in Point Fortin, in southwestern Trinidad, and began protesting outside for a pay raise. The protesting workers were hired by a subcontractor to help build a fourth processing unit at Atlantic's plant, Le Gendre said. Atlantic supplied the United States with about 77 percent of its liquid natural gas imports in 2003, according to Trinidad's ministry of energy.
Source: http://biz.yahoo.com/ap/040211/cb_fin_trinidad_atlantic_lng_2.html

[Return to top]

Chemical Sector

6. *February 12, ThisWeek Newspapers (Columbus, OH)* — **Acid leak ties up area for five hours. A cloud of hydrochloric acid hung over Hilliard, and immediately south of Hilliard, OH, on Tuesday, February 10, when two railroad tanker cars collided at the Buckeye Yard,** 4882 Trabue Road, which houses Norfolk−Southern railroad cars. Roads were closed, some businesses were evacuated and traffic backed up for miles after the spill, which occurred about 10:45 a.m. By 4 p.m. traffic was moving again and clean−up had begun. **The source of the spill and subsequent cloud was believed to be a 23,000−gallon railroad tanker, according to Dan Kochensparger, public information officer for the Upper Arlington Fire Department. As a result of the collision, the tank was knocked off its track and was leaking a solution of muratic acid −− a weak form of hydrochloric acid, according to Kelly McGuire, public information assistant with the Columbus Division of Fire.** Sherri Mercurio, a spokesperson with the Columbus Division of Police, said the evacuation period was brief. Residents weren't allowed within a one−mile radius of the accident, she said. "The area that was evacuated was a business area," she said. There were homes located within two miles of the spill, she said, but the weather cooperated and there was no wind to blow fumes toward residents who might have had to be evacuated.
Source: http://www.thisweeknews.com/thisweek.php?edition=common&story=thisweeknews/021204/hil/News/021204−News−372305.html

7. *February 12, BBC* — **Mystery shrouds Nigeria gas leak. Details are emerging of a chemical gas leak in a suburb of Nigeria's commercial capital, Lagos, on Tuesday, February 10. More than 80 people, including many children and three fireman, were admitted to hospital. The Nigeria Red Cross found that poison gas had escaped from a metal fabricating factory and drifted over three nursery and primary schools.** A Red Cross official told the BBC that the children were choking, vomiting and collapsing in the suburb of Oko Oba. In all, 500 people were affected by the chemical leak. The three schools have now

been closed until next week. The factory has been cordoned off by police and the Red Cross say the owner has been arrested. At least 60 people, including pupils, were admitted to hospital on Tuesday. Police say the situation is now fully under control and that nearly all of the patients have been discharged. It is still not clear what was inside the pressurised canister, which leaked. **A spokesman for the Lagos state government said it was chlorine. The police were less specific, saying only the substance was used for welding iron.** This is not the first accident in Lagos caused by dangerous substances stored in a built−up area.
Source: http://news.bbc.co.uk/2/hi/africa/3483171.stm

[Return to top]

Defense Industrial Base Sector

8. *February 12, Washington Post* — **GAO finds that thousands of defense contractors owe taxes. About 27,000 defense contractors owe about $3 billion in back taxes, but neither the Department of Defense (DoD) nor the Internal Revenue Service has made much use of technology or its legal authority to collect it, according to a General Accounting Office (GAO) report.** Many of those companies continued to collect money under their contracts while paying little or nothing on their tax bills, the GAO said. The report, which will be discussed at a hearing of the Senate Permanent Subcommittee on Investigations on Thursday, concluded that if the agencies had fully used their power to withhold up to 15 percent of contract payments to offset back taxes, the government would have collected about $100 million is fiscal 2002, instead of the $332,000 it did collect. **The problem involves about 10 percent of DoD's contractors and about two percent of the dollars awarded.** However, the amount involved is not negligible, said Subcommittee Senators Coleman and Levin. The missing money includes payroll taxes −− Social Security and Medicare −− as well as income taxes, they said. Report: http://www.gao.gov/new.items/d0495.pdf
Source: http://www.washingtonpost.com/wp−dyn/articles/A35214−2004Feb 12.html

9. *February 11, Technology Daily* — **Pentagon faces challenge in creating armed services information network.** The Department of Defense faces strategic challenges as it works to create a joint information network that allows war−fighters to communicate across the armed services, military officials told lawmakers on Wednesday. **Major General Marilyn Quagliotti, whose division oversees work on joint communication capabilities, told lawmakers that the department must address two problems to create a global network: it must organize the forces to support, and it must view the networks as an integral part of war−fighting and solve inter−branch communications snags.** "Actions must be accomplished in each of these areas for network−centric warfare to become a reality," she said in testimony before the House Armed Services Terrorism, Unconventional Threats and Capabilities Subcommittee. John Stenbit, assistant secretary of defense at the Pentagon's networks and information integration division, said in his testimony that the military's "information vision is to empower users through easy access to information anytime and anyplace, with attendant security." To achieve that goal, the department is employing a global information grid that the department defines as a "globally interconnected."
Source: http://www.govexec.com/dailyfed/0204/021104tdpm1.htm

[Return to top]

Banking and Finance Sector

10. *February 12, Associated Press* — **Countries crack down on scam Websites. Two dozen countries are participating in a three−day crackdown on scam Websites that try to swindle visitors with get−rich−quick and other schemes. The Australian Competition and Consumer Commission is leading consumer protection agencies from the United States, Britain, Canada and other countries on a search this week for sites that make claims "too good to be true,"** commission Deputy Chair Louise Sylvan said. The primary targets are offers that promise a lot but often have large startup fees, added costs and "grossly exaggerated earning potential," the commission said. "The point is to clean it up, to send a strong message that we want consumers to be safe shopping on the Net and that we're out there watching," Sylvan said. The Internet sweep is being conducted through the International Consumer Protection and Enforcement Network of consumer protection authorities from 31 countries. Source: http://seattlepi.nwsource.com/business/aptech_story.asp?category=1700&slug=Scam%20Web%20Sites

[Return to top]

Transportation Sector

11. *February 12, General Accounting Office* — **GAO−04−440T: Airport Security: Challenges to Airport Passenger and Baggage Screening (Testimony).** Testimony before the Subcommittee on Aviation, House Committee on Transportation and Infrastructure on February 12. To assess the progress of passenger and baggage screening operations, the General Accounting Office (GAO) was asked to describe the Transportation Security Administration's (TSA) efforts to (1) hire and deploy passenger and baggage screeners, (2) train the screening workforce, (3) measure screener performance in detecting threat objects, and (4) leverage and deploy screening equipment and technologies. TSA met its mandate to establish a federal screener workforce by November 2002, but continues to face challenges in hiring and deploying passenger and baggage screeners. Staffing shortages at some airports and TSA's hiring process have hindered TSA's ability to fully staff screening checkpoints without using additional measures, such as overtime. **In prior reports, GAO has made numerous recommendations designed to strengthen airport passenger and baggage screening. GAO also has several ongoing reviews related to the issues addressed in this testimony, and will issue separate reports related to these areas at later dates, with additional recommendations as appropriate.** Highlights: http://www.gao.gov/highlights/d04440thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−440T

12. *February 12, CNN* — **BA cancels two flights on threats.** British Airways (BA) has canceled two upcoming flights −− one to Washington and one to Saudi Arabia −− because of a security threat, the airline said. "Following the latest advice from the UK government, British Airways has canceled this Sunday's flight (February 15) BA 223 from London Heathrow to Washington due to security reasons," BA said in a statement Thursday. "In addition following UK government advice the airline has cancelled Monday's flight (February 16) BA 263 from

London Heathrow to Riyadh in Saudi Arabia due to security reasons," the statement said. The nature of the security threat was not disclosed. BA has delayed or canceled Flight 223 several times in the past two months because of U.S. security alerts. Flights to Saudi Arabia also have been canceled previously. **Officials in Britain have refused to say what intelligence prompted them to advise cancellation of the BA flights, but U.S. authorities have spoken of a "specific and credible" terrorist threat to international flights.**
Source: http://www.cnn.com/2004/WORLD/europe/02/12/flights.canceled/ index.html

13. *February 12, New York Times* — **City issues new safety procedures for S.I. Ferry.** New guidelines intended to tighten safety procedures for the Staten Island ferry were announced today, February 12, about four months after one of the large commuter boats plowed into a pier last year, killing 11 people and wounding dozens. Mayor Michael R. Bloomberg and Transportation Commissioner Iris Weinshall released the investigation into the ferry operation by the Global Maritime and Transportation School. The report was commissioned after the Andrew J. Barberi slammed at cruising speed into a maintenance pier near the terminal in Staten Island during a midafternoon run on October 15. **Among the report's recommendations is the formation of a Safety Management System to define lines of authority and communication −− such as between shore−based and ferry personnel −− and develop procedures for the boats, terminals and maintenance and other operations. Based on its assessment, the report also recommended hiring 95 additional staff. A new Bridge Team Management system would involve a rotating pilot house team of three licensed deck officers, with two in the pilot house at all times, and the third officer ensuring supervision, including in emergencies.** It also recommended that the ferry operation upgrade its equipment, including its radar and speed indicators.
Source: http://www.nytimes.com/2004/02/12/nyregion/12CND−FERR.html?ex=1077253200&en=33ed9d454e3ed9a9&ei=5062&partner=GOOGLE

[Return to top]

Postal and Shipping Sector

14. *February 12, Congress Daily* — **Postal Service users, competitors weigh in on changes.** Calling for greater rate−setting flexibility and increased outsourcing for the U.S. Postal Service, representatives of the postal service's largest customers and its largest competitors met Wednesday with postal reform legislators and congressional leaders. The CEOs of the nation's top postal users and the postal service's main competitors were invited to testify Wednesday before the House Government Reform's special panel on postal reform. **In the committee's third postal change hearing in the past two weeks, the private sector representatives agreed that the postal service must be given greater flexibility in setting its rates, and it must have the freedom to respond more rapidly to market changes.** The panel members agreed that the postal service should focus on its core functions of accepting, collecting, sorting, transporting, and delivering physical mail and packages.
Source: http://www.govexec.com/dailyfed/0204/021204cdam1.htm

15. *February 12, Times (New Jersey)* — **Postal biodetection not in budget. The U.S. Postal Service has vowed to install biodetection technology in postal centers across the country, but its request for money to pay for such equipment was not included in the budget**

proposed by the president. The Postal Service plans to take its case to Congress, but postal spokesman Jim Quirk said the agency has committed to installing the biohazard detection and ventilation and filtration equipment. **If the money doesn't come from the federal government, it will come from increased postal rates, Quirk said.** After the 2001 anthrax attacks, Congress gave the Postal Service $587 million to decontaminate buildings and buy and install biohazard detection equipment. But Quirk said the Postal Service spent $971 million on what many described as complicated, unprecedented tasks. For fiscal year 2005, the Postal Service wants to spend $24 million on biohazard detection equipment, $364 million for ventilation and filtration equipment and $7 million to irradiate Washington, DC, mail. The Postal Service announced last year it would place biodetection equipment in 282 mail processing and distribution facilities across the nation.
Source: http://www.nj.com/news/times/index.ssf?/base/news−1/10765821 59123491.xml

[Return to top]

Agriculture Sector

16. *February 12, Reuters* — **Bird flu found at New Jersey live poultry markets. Bird flu has been detected at four live poultry markets in New Jersey, but the strain is not the same as the deadly Asian virus and the findings were not unusual for live poultry markets in the state, the Star−Ledger newspaper reported on Thursday.** The report quoted state officials as saying the strain was H7N2 and stressed it was not known to be harmful to humans. **The strain was the same one detected in Delaware, where a total of 84,000 chickens have been killed since Saturday after the virus was found on two farms.** New Jersey officials said the state typically finds bird flu at 40 percent of the live poultry markets, the Star−Ledger report said.
Source: http://www.agriculture.com/worldwide/IDS/2004−02−12T143830Z_ 01_N12289776_RTRIDST_0_BIRDFLU−NEWJERSEY.html

17. *February 12, Reuters* — **Norway finds bird flu in wild duck.** Norwegian veterinarians said on Thursday tests on a wild duck had found a "benign" version of the bird flu virus sweeping Asia. **Stein Ivar Ormsettroe, a director at the Norwegian Food Safety Authority, said the virus had minor symptoms and was probably not even deadly for the infected bird.** "We don't think it can spread to humans," he said, describing it as a "benign" strain of the virus that has killed at least 19 people in Asia. Veterinarians detected the virus after testing both wild birds and poultry late last year. Authorities revealed the results on Thursday after completing the analysis of the tests. **Veterinarians will investigate the find to determine by February 20 whether to launch a wider testing of birds.**
Source: http://www.alertnet.org/thenews/newsdesk/L12621776.htm

[Return to top]

Food Sector

18. *February 12, PR Newswire* — **Food safety technology. A technology company providing individual−animal tracking, food−safety, and animal information solutions announced that preliminary tests demonstrate that it has technology that is successful in the detection**

of spinal tissue for use in the identification and removal of certain Specified Risk Materials (hazardous materials thought to be responsible for the transmission of bovine spongiform encephalopathy (BSE). "Preliminary tests over the last three months are encouraging, and we are currently in the process of developing a prototype for commercial trials in mid−2004," stated David C. Warren, the company's president and CEO. "Over the next several months, the company plans to define market and technical requirements to modify our existing technology for use in detecting spinal and a number of specified risk material tissues within meat processing plants." The U.S. Department of Agriculture has issued interim rules, which specifically relate to the identification and removal of Specified Risk Material, expand prohibited materials to include dorsal root ganglia, clusters of nerve cells connected to the spinal cord along the vertebral column, in addition to spinal cord tissue, all of which may benefit from enhanced visual inspection methods.
Source: http://www.agprofessional.com/show_story.php?id=23551

[Return to top]

Water Sector

19. *February 10, Associated Press* — **Washington DC to spend millions to eradicate lead.** The District of Columbia Water and Sewer Authority (WASA) announced a number of steps being taken to address elevated lead levels found in some city water samples. The more aggressive action plan follows criticism of initial efforts to inform the public of a threat. **WASA is adding $7 million to the $10 million budgeted to replace lead service lines this year. Of 130,000 WASA service lines, officials estimate that 23,000 contain lead.** The independent authority began experiencing unexplained spikes in some samples in August 2002. Although customers were notified with bill inserts, and free water testing was made available to some property owners, consumers and some elected city officials have said more should have been done. Plans call for WASA to replace at least 1,300 of the lines this year. The agency is also expanding a testing program designed to identify homes where lead levels may exceed 300 parts per billion. Tests from homes not connected to lead service lines typically show lead levels below 15 parts per billion. WASA also plans to test the water at all 167 of the city's public schools beginning Saturday.
Source: http://www.wjla.com/news/stories/0204/125201.html

[Return to top]

Public Health Sector

20. *February 12, Associated Press* — **New human bird flu cases. Thailand confirmed three new human bird flu cases Thursday as health officials warned it could take two years to conquer Asia's outbreak.** Meanwhile, the World Health Organization (WHO) said the latest tests show no sign of a killer hybrid virus that could easily pass between people. Tests on a cluster of bird flu cases in a Vietnamese family showed there was no mixing of genes between the bird flu strain and human flu, according to the WHO. While two of the three people labeled as new cases in Thailand have recovered, the third, a 13−year−old boy, was in intensive care in northeastern Chaiyaphum province, Thai officials said.

Source: http://www.theledger.com/apps/pbcs.dll/article?AID=/20040212 /API/402120814

21. *February 12, Boston Globe* — **Bush seeks major boost for Public Health Service.** The Bush administration plans to seek the largest expansion ever of the U.S. Public Health Service in order to recruit thousands of doctors, nurses, and health officers to respond to national health emergencies, such as bioterrorism threats and new strains of infectious diseases, according to senior administration officials. **The plan would increase the Public Health Service's force of 6,000 uniformed officers by more than 1,000 annually for an unspecified number of years and create a reserve of health care professionals who could be called into service at times of crisis.** A major goal is to transform the federal agency from mainly a provider of medical care to the underprivileged into a front−line defender against threats to the nation's health. Surgeon General Richard H. Carmona, who supervises the Public Health Service, said the White House and Department of Health and Human Services (HHS) are drawing up legislation and identifying other ways to "make the U.S. Public Health Service stronger." **HHS spokesman Craig Stevens said the Bush administration is committed to the expansion but the ultimate size and cost have yet to be determined.**
Source: http://www.boston.com/news/nation/articles/2004/02/12/bush_seeks_major_boost_for_public_health_service/

22. *February 12, Reuters* — **WHO aims boost funding for "poor country" diseases. The World Health Organization (WHO), alarmed at low investment in drugs to tackle Third World diseases, launched a long−promised probe on Thursday into how to remedy the situation.** Ninety percent of the some 14 million deaths a year worldwide from infectious diseases are in poor countries, but few new drugs are being developed to fight them. The launching of the investigation was approved at the WHO's annual assembly last May, but only after a heated debate between states over the role of international patent rights in promoting drugs' research. **Wealthier nations warned any attempt to ensure better and cheaper access to medicines in poorer countries by curtailing intellectual property rights would backfire because pharmaceutical companies would have no incentive to develop new drugs.** Part of the job of the commission will be to examine the role played by patents in the development of medicines. It will also look into how to increase funding for research and production of new medicines. **According to the WHO, some 1,400 new medicines were developed between 1975 and 1999, but only 13 for tropical diseases and only three for tuberculosis, which kills nearly two million people a year.**
Source: http://www.alertnet.org/thenews/newsdesk/L1256053.htm

[Return to top]

Government Sector

23. *February 12, Government Executive Magazine* — **Mayors want more direct homeland security funding.** The federal government should bypass state bureaucracies and provide more money directly to local cities so they can pay for homeland security needs, the chairman of the U.S. Conference of Mayors' Homeland Security Task Force said Wednesday, February 11. In January 2004, the U.S. Conference of Mayors issued its second national survey of 215 major cities showing that up to 90 percent of metropolitan areas had not received any funding from the largest federal programs for first responders. **Secretary of the Department of Homeland**

Security Tom Ridge told Congress this week that up to $9 billion in grants awarded in previous years remains unspent, mainly because states have yet to distribute it to cities and counties. The Baltimore Mayor, Martin O'Malley, acknowledged that some metropolitan areas are not yet organized enough to handle a large infusion of funds, but they need more than the federal government is now providing, especially in the form of direct block grants. O'Malley supports a new plan DHS submitted to Congress last month that will overhaul the government's funding formula for state and local first responders.
Source: http://www.govexec.com/dailyfed/0204/021104c1.htm

24. *February 11, Federal Computer Week* — **HSARPA awards small biz grants.** A total of 66 firms will get grants from the Department of Homeland Security under a research program intended to bring new technologies into the department. **Under the Small Business Innovation Research program, the department's Homeland Security Advanced Research Projects Agency (HSARPA) will award six−month contracts of $100,000 or less to the firms to define the scientific, technical and commercial merit of their ideas.** The 66 companies will get a total of $6.5 million, according to agency officials. Firms that succeed at that will be invited to apply for Phase II awards of up to $750,000, to develop the idea into a prototype. The program is limited to small businesses.
Source: http://www.fcw.com/fcw/articles/2004/0209/web−hsarpa−02−11−0 4.asp

[Return to top]

Emergency Services Sector

25. *February 12, Federal Computer Week* — **Maryland security to boost communication.** Maryland state homeland security officials plan to increase communication between their offices and local governments to fix gaps in information, funding and understanding, the state's homeland security director said today, February 12. **Each state has a different process for coordinating homeland security across all levels of government and within Maryland, the last three months have shown that "we, as a state, have got to get ourselves organized," said Dennis Schrader.** He was speaking at the first meeting of the Homeland Security Leadership Alliance in Baltimore, MD. Schrader joined the governor's homeland security office last year, and a common problem since then has been the question of how to get funding to where it needs to be, since first responders are spread across state, county and city lines. For Maryland, the process is based entirely on reimbursement −− with a city spending the money and applying to the state for reimbursement −− and at the state level, officials have finally decided that "we've got to get into the local jurisdictions and teach them this process," Schrader said.
Source: http://www.fcw.com/geb/articles/2004/0209/web−maryland−02−11 −04.asp

26. *February 12, Firehouse.com* — **Maryland emergency responders participate in terrorism drill.** There was a lot of excitement at the National Naval Medical Center in Bethesda, as hundreds of emergency personnel took part in a simulated mass casualty drill on the grounds of the hospital. Hospital personnel, along with emergency workers from National Institutes for Health (NIH), Montgomery County Fire and Rescue, and firefighters from Bethesda−Chevy Chase and Kensington simulated a mass casualty drill. The purpose of the exercise was to test and evaluate a newly revised disaster plan. "What we are specifically looking at is how we can

coordinate both our external and our internal response capabilities. We rely heavily on our civilian sector as our first responders or our civilian fire department to augment our fire station," said Lt. Chris Gillette. **In the mass casualty drill, emergency workers have to figure out how to treat 18 different patients, some of them with gunshot wounds and others with injuries from a car accident. All of them have potentially been exposed to a dangerous chemical. Decontamination experts say the most important part of the exercise is to get the injured into a decontamination unit as soon as possible.** The drill is one of two simulated exercises that the hospital does each year.
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=17&id=25774

27. *February 12, The News−Record (Gillette, WY)* — **Writing the book on fire safety.** Most people wouldn't look at a raging wildfire and think of ... airline safety. But when Campbell County firefighters Randy Okray and Tom Lubnau went looking for ways to improve firefighters' safety and efficiency, research done by the airline industry was exactly where they turned for ideas. **"When the situation is a high stress situation, when you have a lack of information and life−or−death consequences, people behave predictably," explains Lubnau, who co−authored "Crew Resource Management for the Fire Service," a recently published book on firefighter safety, with Okray. "And if you focus on those behaviors, you can trap human errors," Lubnau continued.** Beyond similarities in the stress levels of environments in which airline pilots and firefighters work, Okray says that much of the research on the two fields is similar. "(In) a lot of the studies, you can take '737' out and 'pilot' out and put in "fire truck" and "command officer;' it's a lot of the same sort of things," Okray says. "Most research shows what's important is nonspecific." **The principle is simple: errors that can lead to firefighting catastrophes aren't always tactical or technical. In fact, more often then not they're problems of psychology or personal communication.**
Source: http://www.gillettenewsrecord.com/articles/2004/02/12/news/n ews06.txt

[Return to top]

Information and Telecommunications Sector

28. *February 12, The Register (UK)* — **Nachi variant wipes MyDoom from PCs. A new variant of the Nachi worm which attempts to cleanse computers infected by MyDoom and download Microsoft security patches to unprotected computers arrived on the Internet Thursday, February 12. Nachi.B (also called Welchi) uses the same security vulnerability exploited by the Blaster worm to spread.** Once it infects target machines the worm attempts to search and destroy any traces of MyDoom infection −− before downloading patches for the Microsoft vulnerability it used to infect the system in the first place. The scanning traffic generated by the original Nachi worm in August 2003 caused huge problems. Anti−virus vendors fear a repeat performance this time around. This concern is compounded by the plethora of new viruses released in recent days. As well as the Doomjuice worms (which target Microsoft's Website in DDoS attacks), we have MyDoom and variants and now a Nachi variant. **Thursday also saw the arrival of a Trojan, called Mitglieder.H, with the ability to spread to computers infected with the MyDoom.A worm.**
Source: http://www.theregister.co.uk/content/56/35524.html

29.

February 12, The Register (UK) — **MyDoom virus ends. MyDoom.A is programmed to stop spreading Thursday, marking the end of arguably the worst e−mail−borne viral epidemic to date.** MessageLabs, the e−mail filtering firm, blocked the virus 43,979,281 times in the two weeks since its first appearance in late January. At the height of the epidemic, one in 12 e−mails the firm scanned were viral. MyDoom.A was programmed to launch a denial of service attack against www.sco.com from infected machines. **Even though MyDoom.A will stop spreading, the back door component of the virus has no time limit; it is still running on virus−ridden PCs. Infected machines still need to be identified and decontaminated.** This is doubly important because the recently−released Doomjuice worm uses this back door access to direct infected machines to packet Microsoft's Website. MyDoom.A infected anything between 400,000 and one million PCs, according to various estimates from anti−virus firms.
Source: http://www.theregister.co.uk/content/56/35516.html

30. *February 12, Associated Press* — **Microsoft source code leaked over Net. Microsoft Corp. said late Thursday that portions of its Windows source code, the blueprint of its dominant computer operating system, had been leaked over the Internet.** Microsoft spokesman Tom Pilla said in an interview with The Associated Press that some incomplete portions of the Windows 2000 and Windows NT4.0 source code had been "illegally made available on the Internet." **Access to the source code could allow hackers to exploit the operating system and attack machines running some versions of Windows.** Several versions of the operating system, including the ones containing leaked code, are used on hundreds of millions of computers worldwide. The company was made aware of the leak Thursday and was investigating, Pilla said. He did not know how much of the code had been leaked, when the leak occurred, or how many people might have gained access to it. The company could not immediately pinpoint the source of the leak, and has contacted law enforcement authorities, he said.
Source: http://apnews.myway.com/article/20040213/D80M57NG1.html

31. *February 11, Federal Computer Week* — **Security chief urges partnering.** A Department of Homeland Security (DHS) official said on Wednesday that the government's record of fostering public/private partnerships for securing cyberspace needs to improve. **While claiming progress on cybersecurity, Amit Yoran, director of the National Cyber Security Division at DHS, vowed that the government would work harder on developing its relationships with the private sector in the coming year and would also pursue a long−term agenda that may not see results for many years to come.** Yoran said that while DHS is focused "on changing the fundamental ground rules of cybersecurity," it also has more immediate tasks on its agenda, such as building what he described as a survivable network for sharing critical information if the Internet and other communications systems are brought down by an attack. Yoran said that DHS will be thinking of cybersecurity in broad terms and trying to avoid a too−narrow focus on cyberterrorism. For that reason, he said, **many of the government's long−term cybersecurity efforts will be to improve practices used within the software industry to develop and evaluate software code, in part by using more automated techniques for writing secure software.**
Source: http://www.fcw.com/fcw/articles/2004/0209/web−yoran−02−11−04 .asp

Current Alert Levels

 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_MYDOOM.A** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	3127 (mydoom), 135 (epmap), 137 (netbios−ns), 1434 (ms−sql−m), 445 (microsoft−ds), 80 (www), 1080 (socks), 6129 (dameware), 3128 (squid−http), 4000 (Connect−BackBackdoor) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

32. *February 13, CNN* — **Soldier held on suspicion of espionage. A National Guard soldier at Fort Lewis, Washington, was arrested Thursday on suspicion of trying to pass information about military capabilities to the al Qaeda terrorist organization, military officials said.** Spc. Ryan G. Anderson, 26, was taken into custody following an internal sting operation, said Lt. Col. Stephen Barger, post spokesman. **He will be charged with "aiding the enemy by wrongfully attempting to communicate and give intelligence to the al Qaeda terrorist network," Barger said.** Barger said the investigation involved the Army, the FBI, and the Justice Department. Barger said it could be four or five days before charges are formally filed.
Source: http://www.cnn.com/2004/US/02/12/natl.guard.espionage/

33. *February 12, Reuters* — **U.S. probes South Africa nuclear black market link. Washington has sent investigators to South Africa, a former atomic power, to probe a possible link to an illicit network in nuclear technology following the arrest of a Cape Town man in the United States.** South African police said on Thursday, February 12, that Washington had asked for their help in investigating possible associates of Asher Karni, a former Israeli army officer accused by the U.S. government of conspiring to export 200 U.S.−made nuclear weapons detonators to Pakistan via South Africa. U.S. federal agents arrested Karni, who has lived in South Africa for the last 18 years, when he arrived at Denver International Airport on January 1. Prosecutors say Karni, using an American broker, acquired nuclear triggering devices from their manufacturer in the United States after falsely representing they were destined for a South African hospital. **U.S. Justice Department official Channing Phillips said U.S. authorities had reason to believe Karni had other associates.** "If you look at the (charge) documents you will see the link between his domicile there with what he is alleged to have done and why we

are really interested in his associations there in South Africa," he said.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2004_02_12_eng-reuters_pma_U-S-PROBES-S-AFRICA-NUCLEAR-BLACK-MARKET-LINK&SMContentSet=0

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings - DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications - DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive - Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883-3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-3644 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323-3204.

DHS/IAIP Disclaimer